JASON R. HULL [11202]
JHULL@MOHTRIAL.COM
TREVOR C. LANG [14232]
TLANG@MOHTRIAL.COM
MARSHALL OLSON & HULL, PC
NEWHOUSE BUILDING
TEN EXCHANGE PLACE, SUITE 350
SALT LAKE CITY, UTAH 84111
TELEPHONE: 801.456.7655

ATTORNEYS FOR PLAINTIFF AND
PROPOSED CLASS COUNSEL

GARY M. KLINGER*
GKLINGER@MILBERG.COM
JOHN J. NELSON*
JNELSON@MILBERG.COM
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC**
227 W. MONROE STREET, SUITE 2100
CHICAGO, IL 60606
TELEPHONE: (866) 252-0878
*PRO HAC VICE FORTHCOMING

**IN THE UNITED STATES DISTRICT COURT**
**DISTRICT OF UTAH, CENTRAL DIVISION**

| | |
|---|---|
| BRUCE BISCHOFF, an individual on behalf of himself and all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>C.R. ENGLAND, INC., a Utah Corporation,<br><br>Defendant. | **COMPLAINT**<br><br>**[PROPOSED CLASS ACTION]**<br><br>**JURY TRIAL DEMANDED**<br><br>Case No.: 2:28-cv-00388-DAO |

Plaintiff Bruce Bischoff ("Plaintiff" or "Bischoff"), individually and on behalf of all others similarly situated, brings this action against Defendant C.R. England, Inc. ("CRE" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

## NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyber-attack against CRE that

allowed a third party to access CRE's computer systems and data, resulting in the compromise of highly sensitive personal information belonging to tens of thousands of current and former students, employees, and independent contractors (the "Cyber-Attack").

2. As a result of the Cyber-Attack, Plaintiff and Class Members suffered ascertainable injury and damages in the form of the substantial and present risk of fraud and identity theft from their unlawfully accessed and compromised private and confidential information (including Social Security numbers), lost value of their private and confidential information, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. Plaintiff's and, on information and belief, approximately 224,572 Class Members' sensitive personal information—which was entrusted to Defendant, their officials and agents—was compromised, unlawfully accessed, and stolen due to the Cyber-Attack and subsequent data breach (the "Data Breach"). Information compromised in the Cyber-Attack includes at least the following: full names, addresses, dates of birth, and Social Security numbers (collectively the "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

5. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant CRE's computer network in a condition vulnerable to cyber-attacks of this type.

6. Upon information and belief, the mechanism of the Cyber-Attack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known and

foreseeable risk to Defendant, and Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. The Cyber-Attack occurred in October 2021 but Defendant was unable to ascertain that Plaintiff's information was compromised until April, 2022. Had Defendant properly monitored their property and custodied information, they would have discovered the extent of the intrusion sooner which would have allowed Plaintiff and Class Members to sooner mitigate the effects thereof.

8. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

9. Armed with the Private Information accessed in the Cyber-Attack, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. As a further result of the Cyber-Attack, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Plaintiff and Class Members have and may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. As a direct and proximate result of the Cyber-Attack and subsequent Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of: 1) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach; and 2) charges, and fees charged against their accounts. Plaintiff and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own personally identifying information ("PII") such that they are entitled to damages for unauthorized access to and misuse of their PII from Defendant, and Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their PII as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

13. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Cyber-Attack.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiff brings this action against Defendant seeking redress for their unlawful conduct asserting claims for negligence, negligence *per se*, breach of implied contract, and violation of the consumer protection statutes invoked herein.

## PARTIES

16. Bischoff is an individual citizen of the State of Nevada residing in Las Vegas, Cook County, Nevada. Plaintiff Bischoff began commercial driver's training with CRE in or around June 2009. In or about November 2009, Plaintiff was employed by CRE as a commercial freight driver. Thereafter, Plaintiff Bischoff became an independent contractor driving commercial freight for CRE. As a condition of his initial training, his employment with CRE, and his transition to independent contractor, he was required to provide his Private Information. On or about May 23, 2022, Plaintiff Bischoff received notice from Defendant that the Data Breach had occurred following "unauthorized access to certain files stored within our systems," and that his personal data (including his name, address, date of birth, and Social Security number) were involved. According to the letter, CRE had discovered this breach seven months prior, in October of 2021.

17. CRE is a Utah corporation with its principal place of business at 4701 W. 2100 South, Salt Lake City, Salt Lake County, Utah 84120.

## JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is in the tens of thousands, many of whom have different citizenship from Defendant, including the named Plaintiff here. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has jurisdiction over the Defendant because it operates and/or is incorporated in this District, and the computer systems implicated in this Data Breach are likely based in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendant is based in this District, maintains Class Members' PII in the District and has caused harm to Class Members residing in this District.

## FACTUAL ALLEGATIONS

### *Defendant's Business*

21. CRE is a trucking driving school and commercial freight carrier, based in Salt Lake City, Salt Lake County, Utah.

22. CRE trains students to obtain commercial freight driver's credentials and employs drivers to haul commercial freight across the country. Defendant also contracts with independent drivers to haul commercial goods to and from destinations nationwide.

23. CRE has other truck driving school locations in Colton, California; Laredo, Texas; and Valparaiso, Indiana.

24. In the ordinary course of doing business with Defendant, current and former employees provide Defendant with sensitive, personal, and private information such as:

- Name;
- Address;
- Phone number;
- Driver's license number;

- Social Security number;
- Date of birth;
- Email address;
- Gender.

25. On information and belief, in the course of collecting Private Information from current and former employees, including Plaintiff, Defendant promised to provide confidentiality and adequate security for employee data through their applicable privacy policy and through other disclosures.

26. Plaintiff and Class Members, as current and former students, employees, and independent contractors, relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Due to its sensitive nature and the consequences to individuals for its misappropriation, Plaintiff and Class Members demand security to safeguard their PII.

27. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

***The Cyber-Attack and Data Breach***

28. On or about May 23, 2022, Defendant CRE began notifying current and former students, employees, and independent contractors and state Attorneys General about a data breach that was discovered on or about October 30, 2021 (the "Data Breach").

29. According to the Notice of Data Security Incident letters, and letters sent to state Attorneys General, CRE "discovered unauthorized activity on our systems" on or about October 30, 2021, and that an "there was unauthorized access to certain files stored within our systems."

CRE subsequently determined, only on April 20, 2022, that Plaintiff's full name, date of birth, addresses, and social security number were compromised as a result of the Data Breach.

30. On May 23, 2022 Plaintiff Bischoff was informed that his full name, address, date of birth, and Social Security number were among the data "taken" in the Data Breach.

31. Due to the severity of the Data Breach, Defendant offered consumers "twelve (12) months of complimentary identity theft monitoring services through IDX [...]"

32. Based on the Notice of Data Breach letter he received, which informed Plaintiff that his Private Information was accessed and "taken" on Defendant's network and computer systems, Plaintiff believes his name, address, date of birth, and Social Security number were stolen from Defendant's network and potentially sold or published on the Dark Web.

33. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

34. Indeed, Defendant's own Privacy Policy warrants that CRE "recognizes the importance of protecting information and data [it] collects." Moreover, CRE's Privacy Policy promises to "safeguard the information and data [potential employees] provide to [C.R. England] from unauthorized access and unauthorized disclosure . . ."[1]

35. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

[1] https://www.crengland.com/about-us/privacy-policy#:~:text=and%20online%20policies.-,C.R.,practices%20relating%20to%20those%20websites.

36. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

37. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[2] These incidents continue to rise in frequency, with an estimated 1,862 data breaches occurring in 2021.[3]

38. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

***Defendant Failed to Comply with FTC Guidelines***

39. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

40. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

[2] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Ye ar-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 10, 2020).

[3] https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/

understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

41. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

42. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

43. Defendant failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

44. Defendant was at all times fully aware of its obligation to protect the Private Information of customers and prospective customers. Defendant was also aware of the significant

repercussions that would result from its failure to do so.

***Defendant Failed to Comply with Industry Standards***

45. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing and implementing Defendant's cybersecurity practices.

46. Best cybersecurity practices that are standard in industries that custody private and protected information include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

47. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

48. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the Cyber-Attack and causing the data breach.

***Defendant's Breach***

49. Defendant breached its obligations to Plaintiff and Class Members and/or was

otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, networks, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect current and former employees' Private Information;

c. Failing to adequately protect Private Information of current and former employees' family members;

d. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

e. Failing to apply all available security updates;

f. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

g. Failing to practice the principle of least-privilege and maintain credential hygiene;

h. Failing to avoid the use of domain-wide, admin-level service accounts;

i. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

j. Failing to properly train and supervise employees in the proper handling of inbound emails.

50. As the result of computer systems in need of security upgrading and inadequate

procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

***Data Breaches Cause Disruption and Put Victims at an Increased Risk of Fraud and Identity Theft***

51. Defendant understood the Private Information it collected is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the cyber-criminals who perpetrated this Cyber-Attack.

52. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

53. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven (7) years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[5]

54. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

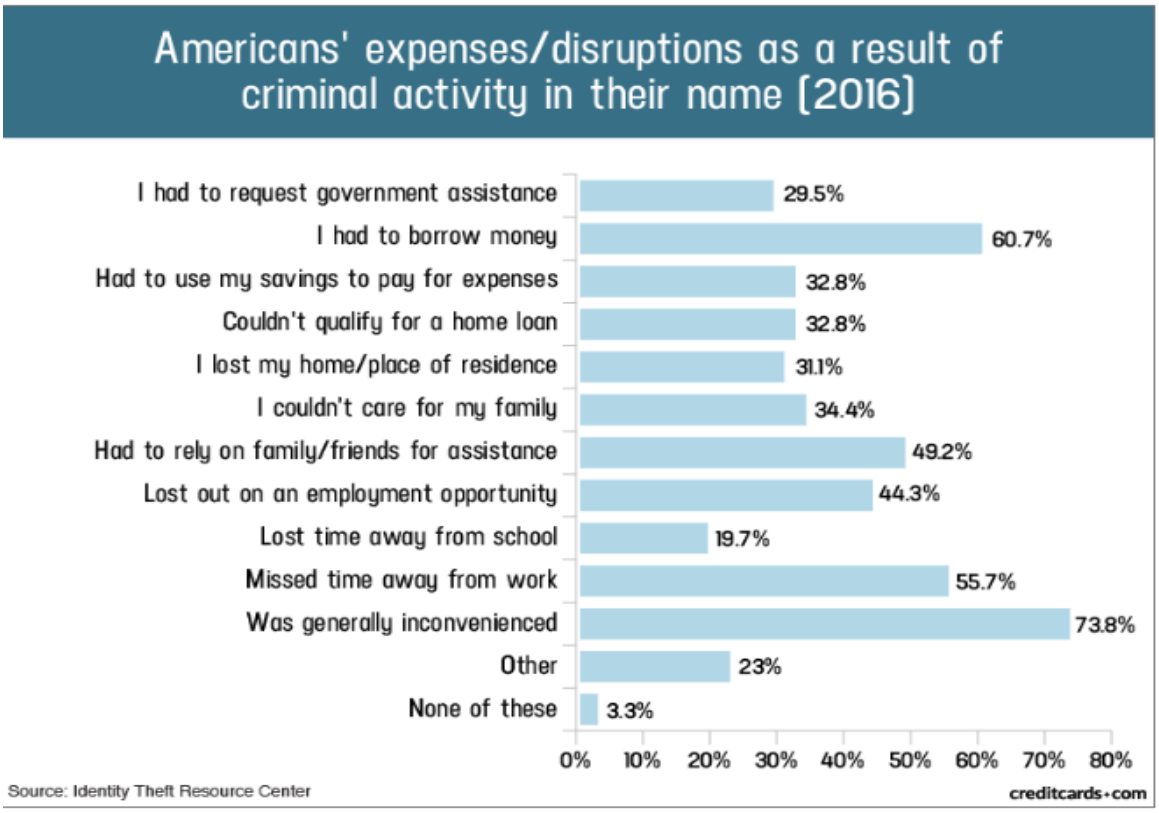
55. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name

[4] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").
[5] *See* https://www.identitytheft.gov/Steps (last visited Dec. 8, 2020).

and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

56. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

57. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[6]




[6] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed Dec. 10, 2020).

58. What's more, theft of Private Information is also gravely serious. PII is a valuable property right.[7]

59. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

60. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

*See* GAO Report at 29.

61. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

62. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites.

63. Where the most private information belonging to Plaintiffs and Class Members was

[7] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

accessed and removed from Defendant's network, there is a strong probability that the stolen information is yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

64. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

65. Sensitive information can sell for as much as $363 according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

66. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.

67. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

68. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used

to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

69. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[8]

70. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[9]

71. At all relevant times, Defendant knew or reasonably should have known these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached and strengthened their data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

[8] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Oct. 28, 2020).

[9] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 28, 2020).

***Plaintiff's and Class Members' Damages***

72. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Cyber-Attack and Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Cyber-Attack. Defendant has only offered 12 months of inadequate identity monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen) or to all persons whose data was compromised in the Cyber-Attack.

73. Moreover, the 12 months of credit monitoring offered to persons whose private information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

74. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

75. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Cyber-Attack. Moreover, Defendant's delay in noticing affected persons of the theft of their PII prevented early mitigation efforts and compounded the harm.

***Plaintiff's Experience***

76. Plaintiff Bischoff provided his PII to CRE as a condition of his employment with CRE. Plaintiff Bischoff also provided his PII to CRE as a condition of his enrollment in CRE's commercial driver training course and as part of his transition to independent contractor driving freight contracts for CRE.

77. On or about May 23, 2022, Plaintiff received a "Notice of Data Security Incident"

letter from CRE informing him that his full name, address, date of birth, and social security number were stolen by cyberthieves in the Data Breach.

78. As a result of the Data Breach, CRE directed Plaintiff to take certain steps to protect his PII and otherwise mitigate his damages.

79. As a result of the Data Breach and the information that he received in the Notice Letter, Plaintiff spends approximately 2-3 hours per week dealing with the consequences of the Data Breach (self-monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the *Notice of Data Security Incident*, communicating with his bank, ensuring accounts are locked, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

80. Plaintiff is very careful about sharing his own PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

81. Plaintiff stores any and all documents containing PII in a secure location, and destroys by shredder any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts to maximize his digital security efforts.

82. Plaintiff suffered actual injury and damages due to Defendant's mismanagement of his PII before the Data Breach.

83. Plaintiff suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of providing him payroll and benefit services, which was compromised in and as a result of the Data

Breach.

84. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered anxiety and increased concerns for the theft of his privacy since he received the Notice Letter. He is especially concerned about the theft of his full name paired with his Social Security number, address, and date of birth.

85. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

86. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

## CLASS ACTION ALLEGATIONS

87. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

88. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure 23.

89. Plaintiff proposes the following Class definition(s), subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Class:

> All persons whose Private Information was compromised as a result of the Cyber-Attack that CRE discovered on or about October 30, 2021, and who were sent notice of the Data Breach (the "Class").

90. Plaintiff also proposes the following subclass, subject to amendment based on

information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Subclass:

> All persons who paid for trucking schools services and whose Private Information was compromised as a result of the Cyber-Attack that CRE discovered on or about May 20, 2021, and who were sent notice of the Data Breach (the "Student Subclass").

Excluded from the Class and Subclass are members of the judiciary to whom this case is assigned, their families and members of their staff.

91. Plaintiff reserves the right to amend the definitions of the Class or Subclass or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

92. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

93. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of 224,572 of Defendant's current and former students, employees, and independent contractors whose data was compromised in the Cyber-Attack and Data Breach.

94. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Cyber-Attack;

c) Whether Defendant's data security systems prior to and during the Cyber-Attack complied with applicable data security laws and regulations;

d) Whether Defendant's data security systems prior to and during the Cyber-Attack were consistent with industry standards;

e) Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f) Whether Defendant breached their duty to Class Members to safeguard their Private Information;

g) Whether computer hackers obtained Class Members' Private Information in the Cyber-Attack;

h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j) Whether Defendant's conduct was negligent;

k) Whether Defendant breach an implied contract between it and the Plaintiffs;

l) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

95. Typicality. Plaintiff's claims are typical of those of other Class Members because

Plaintiff's information, like that of every other Class Member, was compromised in the Cyber-Attack.

96. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class and has no interests antagonistic to those of other Class Members. Plaintiff's Counsel are competent and experienced in litigating data breach class actions.

97. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

98. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

99. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

**FIRST CLAIM FOR RELIEF**
**Neglience**
**(On Behalf of Plaintiff and All Class Members)**

100. Plaintiff re-alleges and incorporates by reference each preceding paragraph as if fully set forth herein.

101. Defendant required Plaintiff and Class Members to submit non-public personal information as a condition of employment, prior to their status as independent contractor, or to participate in truck diving education courses.

102. By collecting and storing this data in its computer property, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

103. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

104. Defendant's duty of care to use reasonable security measures arose because Defendant was able to ensure that its systems were sufficient to protect against the foreseeable risk

of harm to Class Members from a data breach.

105. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

106. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Cyber-Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

107. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

108. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

109. Had Plaintiff and members of the Class known that Defendant would not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

110. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack and data breach.

111. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face, entitling them to damages in an amount to be proven at trial..

112. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide

adequate credit monitoring to all Class Members.

**SECOND CLAIM FOR RELIEF**
**Negligence Per Se**
**(On Behalf of Plaintiff and the Class)**

113. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 99 above as if fully set forth herein.

114. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

115. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

116. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

117. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

118. Had Plaintiff and Class Members known that Defendant would not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

119. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

120. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

121. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

122. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

**THIRD CLAIM FOR RELIEF**
**Breach of Implied Contract**
(On Behalf of Plaintiff and the Class)

123. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

124. Defendant required Plaintiff and the Class to provide their personal information, including name, address, date of birth, and Social Security number, as a condition of their employment or training courses, or to be eligible as an independent contractor.

125. As a condition of their employment, training, or status as an independent contractor with Defendant, Plaintiff and the Class provided their personal and financial information. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been

breached and compromised or stolen.

126. Defendant offered to provide goods and services to members of the Class who were trucking school students in exchange for payment. Defendant also required the members of the Class who were students to provide Defendant with their PII to receive services and training.

127. Class members who are employees accepted Defendant's offer of employment by providing their PII to Defendant.

128. Class members who are independent contractors accepted Defendant's provision of freight contracts by providing their PII to Defendant.

129. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

130. Had Plaintiff and Class Members known that Defendant would not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

131. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the data breach.

132. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the

compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm, entitling them to damages in an amount to be proven at trial.

**FOURTH CLAIM FOR RELIEF**
**Breach of Implied Covenant of Good Faith and Fair Dealing**
**(On Behalf of Plaintiff and the Class)**

133. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

134. As a condition of their employment, training, or status as an independent contractor with Defendant, Plaintiff and the Class provided their personal and financial information. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

135. Defendant offered to provide goods and services to members of the Class who were trucking school students in exchange for payment. Defendant also required the members of the Class who were students to provide Defendant with their PII to receive services and training.

136. Class members who are employees accepted Defendant's offer of employment by providing their PII to Defendant.

137. Class members who are independent contractors accepted Defendant's provision of freight contracts by providing their PII to Defendant.

138. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

139. Had Plaintiff and Class Members known that Defendant would not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

140. CRE represented to its students, employees, and independent contractors, implicitly and otherwise, that their PII would be secure. Plaintiff and members of the proposed Class relied on such representations when they agreed to provide their PII to C.R. England. Plaintiff and the members of the Class would not have entrusted their PII to Defendant without such agreement with Defendant.

141. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

142. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

143. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

144. Defendant's duty to safeguard Plaintiff's and Class Member's PII is inherent in and consistent with the contracts entered into by CRE and Plaintiff and Class Members.

145. Defendant would not have suffered harm by enacting industry standard measures to safeguard Plaintiff's and Class Member's PII.

146. Defendant's failure to enact reasonable safeguards to protect the PII it collected resulted in harm to Plaintiff and Class Members and violated the covenant of good faith and fair dealing. Similarly, Defendant's failure to timely discover the breach, to timely notify affected persons, and to fully detail the scope of the breach in the "Notice of Data Security Incident," each suffices to demonstrate a breach of the covenant.

147. Plaintiff and Class Members have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

148. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract of good faith and fair dealing, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs in addition to all other damages or relief allowed by law.

## FIFTH CLAIM FOR RELIEF
### Invasion of Privacy
### (On Behalf of Plaintiff and the Class)

149. Plaintiff incorporates all preceding paragraphs as if fully set forth below.

150. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to and access by unauthorized third parties.

151. Defendant owed a duty to its students, employees, and independent contractors, including Plaintiff and the Class, to keep this information confidential.

152. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

153. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant to receive trucking training services and employment, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

154. Had Plaintiff and members of the Class known that Defendant would not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

155. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

156. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

157. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

158. Acting with knowledge, Defendant had notice and knew that its inadequate

cybersecurity practices would cause injury to Plaintiff and the Class.

159. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

160. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

161. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages alone will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

162. In addition to injunctive relief, Plaintiff, on behalf of himself and the other members of the Class, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs in addition to all other damages or relief allowed by law.

## SIXTH CLAIM FOR RELIEF
### Unjust Enrichment
(On Behalf of Plaintiff and all Student Subclass Members)

163. Plaintiff incorporates all preceding paragraphs as if fully set forth below.

164. This claim is pleaded in the alternative to Counts III and IV.

165. Plaintiff and members of the Student Subclass conferred a benefit upon Defendant in the form of monies paid for trucker training services, through employment, and through

provision of services as independent contractors.

166. Defendant appreciated or knew about the benefits conferred upon itself by Plaintiff and members of the Subclass. Defendant also benefited from the receipt of Plaintiff's and members of the Subclass's PII, as this was used to facilitate employment processing, payroll, benefits, and trucker training services.

167. As a result of Defendant's conduct, Plaintiff and members of the Class who are former or current trucking students suffered actual damages in an amount equal to the difference in value between their training cost payments made with reasonable data privacy and security practices and procedures that Plaintiff and members of the Class paid for, and those training cost payments made without unreasonable data privacy and security practices and procedures that they received.

168. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Subclass's payments and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII, nor used and paid for Defendant's goods and services had they known Defendant would fail to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and members of the Subclass paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

169. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Subclass all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than five (5) years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, nominal damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on all triable issues.

DATED this 8th day of June, 2022.

**MARSHALL OLSON & HULL, PC**

BY: /s/ Jason R. Hull
JASON R. HULL
TREVOR C. LANG

**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
GARY M. KLINGER
JOHN J. NELSON

ATTORNEYS FOR PLAINTIFF AND
PROPOSED CLASS COUNSEL